OFFENDER ACCESS TO ELECTRONIC NETWORK
NOTIFICATION OF ACCEPTABLE USE

State of Oregon
OREGON YOUTH AUTHORITY

Electronic networks are specific computers, hardware, software, storage media, and networks accessible to authorized OYA offenders within OYA facilities. Electronic networks provide offenders access to education and employment information to assist in their successful reintegration from confinement into the community.

This document serves to notify offenders of acceptable electronic network use.

- Offender access to the electronic network is for a limited educational purpose. The term "educational purpose" includes classroom activities, career development, and limited transitional activities.
- The OYA electronic network is not a public access service or a public forum. OYA has the right to place reasonable restrictions on material accessed or posted throughout the network.
- An offender must receive written authorization from an OYA manager prior to accessing an electronic network. Access is a privilege; not a right.
- OYA may monitor all activity on the electronic network.
- Offenders are expected to follow the same rules, good manners and common sense guidelines that are used during other education activities.

General Unacceptable Behavior
The following behaviors are unacceptable when using any part of the electronic network:

- Posting information that, if acted upon, could be dangerous or disruptive;
- Harassing another person; or acting in a way that bothers or annoys another person;
- Knowingly or carelessly posting false or insulting information about a person or organization;
- Using criminal speech or speech in the course of committing a crime such as threats to an individual, instructions on breaking into computer networks, child pornography, drug dealing, purchasing alcohol, gang activities, etc;
- Using inappropriate speech for an educational setting;
- Abusing network resources such as sending chain letters or "spamming";
- Displaying or sending offensive messages or pictures;
- Offering, providing, or purchasing items or services through the network;
- Attempting to access unauthorized systems, such as offender information systems or business systems;
- Using any wired or wireless network (including third party Internet service providers) with equipment brought from home. For example, using a home computer on the network or accessing the Internet from any device not owned by OYA.
- Using the electronic network to send or post e-mail that is abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

Electronic Mail (e-mail)

- You may be provided an e-mail account for specific educational or employment-seeking projects or activities.
- Your e-mail account must be approved in advance by the facility superintendent or camp director.
- An OYA staff member or school personnel must log you onto the e-mail account. You cannot have direct access to the e-mail account.
- Your e-mail is monitored.

World Wide Web

Access to information on the Web will generally be provided through prescreened sites according to your facility.

Real-time, Interactive Communication Areas

Access to real-time, interactive communication must be approved in advance by the facility superintendent or camp director; only be provided under the direct supervision of an OYA staff or school personnel; and be for educational or employment-seeking purposes.

Oregon Youth Authority Safety

You must promptly disclose to OYA staff or school personnel any communication received or Web site visited that you think may be inappropriate or an unacceptable use of the Internet. This includes communication or Web site visiting you may have made by mistake.

System Security

- You are responsible for your individual account and must take all reasonable precautions to prevent others from being able to use it. Under no conditions may you provide your password to another offender.
- You must immediately notify OYA staff or school personnel if you think you have a possible security problem. You should not try to fix security problems because this may be interpreted as an illegal attempt to gain access.
- You must not attempt to gain unauthorized access to any part of the electronic network. This includes attempting to log in through another person's account or access another person's folders, work, or files. These actions are prohibited, even if you are only "browsing."
- Do not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means.
- Do not try to access Web sites blocked by OYA, including the use of proxy services, software, or Web sites.
- Do not use sniffing or remote access technology to monitor the network or another user's activity.

Software and Files

- Software is available as an educational resource. Do not install, upload or download software without permission from the OYA Information Systems department.
- Your account may be restricted or terminated if you intentionally misuse software.
  - Files stored on the network are treated the same as other school storage areas, like lockers. Routine network maintenance and monitoring may reveal an unacceptable use of the network. Know that your files stored on the network are not private.

Technology Hardware

Hardware and peripherals are provided as educational or employment-seeking tools. You are not allowed to move hardware, install peripherals or modify settings to equipment without consent from the OYA Information Systems department.

Vandalism

Any malicious attempt to harm or destroy data, the network, other network components connected to the network backbone, hardware or software will result in immediate cancellation of your network privileges.

Plagiarism and Copyright Infringement

- Do not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were your own.
- Copyrighted material must not be placed on any system without the author's permission. Permission may be specified in the document, on the system or obtained directly from the author.

Youth Offender Rights

- An individual search and investigation will be conducted if there is reasonable suspicion that you have violated this notification or related rules. The investigation will be reasonable and related to the suspected violation.
- Any behavior violation associated with your electronic network use must be managed according to OAR chapter 416, division 470 (Prohibited Offender Behaviors and Processing Behavior Violations).

I have read or had read to me this Offender Access to Electronic Network Notification of Acceptable Use and understand the information in this notification.

_____	_____	_____
Offender name, JJIS #	Offender signature	Date

_____	_____
Staff member presenting notification name, title	Date